IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Hugh Svendsen et al.	Examiner: Jung W. Kim
Serial No. 10/813,839	Art Unit: 2132
Filed: 03/31/2004	

For: **METHOD AND SYSTEM FOR PROVIDING WEB BROWSING THROUGH A FIREWALL IN A PEER TO PEER NETWORK**

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

An **APPEAL BRIEF** is filed herewith. The Appellants enclose a payment in the amount of $510.00 as required by 37 C.F.R. § 1.17(c). If any additional fees are required in association with this appeal brief, the Director is hereby authorized to charge them to Deposit Account 50-1732, and consider this a petition therefor.

APPEAL BRIEF

(1) REAL PARTY IN INTEREST

The present application is owned by Qurio Holdings, Inc. whose corporate headquarters are 1130 Situs Court, Suite 216, Raleigh, NC 27606.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of the Appellants' knowledge.

(3) STATUS OF CLAIMS

Claims 1-34 were rejected with the rejection made final on March 14, 2008.

Claims 10-14 and 26-30 were deemed allowable in the Final Office Action mailed March 14, 2008 if rewritten in independent form; however, the Appellants have not rewritten these claims in independent form.

Claims 1-34 are pending and are the subject of this appeal.

(4) STATUS OF AMENDMENTS

All amendments have been entered to the best of the Appellants' knowledge. No amendments have been filed after the Final Office Action mailed March 14, 2008.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

In the following summary, the Appellants have noted where in the Specification certain subject matter exists. The Appellants wish to point out that these citations are for demonstrative purposes only and that the Specification may include additional discussion of the various elements, citations to which are not pointed out below. Thus, the noted citations are in no way intended to limit the scope of the pending claims.

The present invention provides a method and system for providing a computer running a Web browser with HTTP access to a peer server located behind a firewall in a peer-to-peer network. (Specification, paragraph 007). Particularly, a proxy server multiplexes Web traffic between a firewall-protected peer server and a peer server that is not protected by the firewall. (Specification, paragraph 020). According to the present invention, in response to a proxy server receiving an HTTP request to access the peer server located behind the firewall from the web browser, the HTTP request is translated into a request packet and the request packet is sent to the peer server. (Specification, paragraph 007). In response to the peer server behind the firewall receiving the request packet, the peer server translates the request packet back into the HTTP request and then responds to the request, thereby enabling generic web traffic to flow. (Specification, paragraph 007).

Independent claim 1 recites a method for providing a Web browser (Specification, paragraph 018; see also Figure 2, element 30) running on a computer (Specification, paragraph 018; see also Figure 2, element 32) with HTTP access to a peer server (Specification, paragraph 019; see also Figure 2, element 24') located behind a firewall (Specification, paragraph 019; see also Figure 2, element 34) in a peer-to-peer network (Specification, paragraph 019; see also Figure 2, element 22), comprising;

(a) providing the peer-to-peer network with a proxy server (Specification, paragraph 020; see also Figure 2, element 36);

(b) registering an outbound socket connection with the proxy server by the peer server (Specification, paragraph 021; see also Figure 3, step 50);

(c) in response to the proxy server receiving an HTTP request to access the peer server from the Web browser, translating the HTTP request into a request packet and sending the request packet to the peer server (Specification, paragraph 021; see also Figure 3, step 54); and

(d) in response to the peer server receiving the request packet, translating the request packet back into the HTTP request and responding to the request, thereby enabling generic web traffic to flow (Specification, paragraph 021; see also Figure 3, steps 56, 58, and 60).

Independent claim 17 recites a computer-readable medium containing program instructions for providing a Web browser (Specification, paragraph 018; see also Figure 2, element 30) running on a computer (Specification, paragraph 018; see also Figure 2, element 32) with HTTP access to a peer server (Specification, paragraph 019; see also Figure 2, element 24') located behind a firewall (Specification, paragraph 019; see also Figure 2, element 34) in a peer-to-peer network (Specification, paragraph 019; see also Figure 2, element 22), the program instructions for;

(a) providing the peer-to-peer network with a proxy server (Specification, paragraph 020; see also Figure 2, element 36);

(b) registering an outbound socket connection with the proxy server by the peer server (Specification, paragraph 021; see also Figure 3, step 50);

(c) in response to the proxy server receiving an HTTP request to access the peer server from the Web browser, translating the HTTP request into a request packet, and sending the request packet to the peer server (Specification, paragraph 021; see also Figure 3, step 54); and

(d) in response to the peer server receiving the request packet, translating the request packet back into the HTTP request and responding to the request, thereby enabling generic web traffic to flow (Specification, paragraph 021; see also Figure 3, steps 56, 58, and 60).

Independent claim 33 recites a method for providing a web browser (Specification, paragraph 018; see also Figure 2, element 30) with HTTP access to a peer server (Specification, paragraph 019; see also Figure 2, element 24') located behind a firewall (Specification, paragraph 019; see also Figure 2, element 34) in a peer-to-peer network (Specification, paragraph 019; see also Figure 2, element 22), comprising:

(a) registering an outbound socket connection from the peer server to a proxy server (Specification, paragraph 021; see also Figure 2, element 36);

(b) redirecting all incoming HTTP requests intended for the peer server to the proxy server (Specification, paragraph 021; see also Figure 3, step 52);

(c) in response to the proxy server receiving one of the redirected HTTP request, finding the socket connection to the peer server (Specification, paragraph 021; see also Figure 3, step 54), translating the HTTP requests into a multiplexed protocol comprising a request packet, and sending the request packet to the peer server (Specification, paragraph 021; see also Figure 3, step 54);

(d) in response to the peer node receiving the request packet, demultiplexing the request, translating the request packet back into the original HTTP request, and passing the HTTP request to a local web server (Specification, paragraph 021; see also Figure 3, step 56);

(e) in response to the peer node receiving an HTTP response from the Web server, translating the HTTP response into a response packet, and sending the response packet to the proxy server over the outbound socket connection (Specification, paragraph 021; see also Figure 3, step 58); and

(f) in response to the proxy server receiving the response packet from the peer server, translating the response packet back into the HTTP response, and sending the HTTP response to the requesting Web browser (Specification, paragraph 021; see also Figure 3, step 60).

Independent claim 34 recites a computer-readable medium containing program instructions for providing a web browser (Specification, paragraph 018; see also Figure 2, element 30) with HTTP access to a peer server (Specification, paragraph 019; see also Figure 2, element 24') located behind a firewall (Specification, paragraph 019; see also Figure 2, element 34) in a peer-to-peer network (Specification, paragraph 019; see also Figure 2, element 22), the program instructions for:

(a) registering an outbound socket connection from the peer server to a proxy server (Specification, paragraph 021; see also Figure 2, element 36);

(b) redirecting all incoming HTTP requests intended for the peer server to the proxy server (Specification, paragraph 021; see also Figure 3, step 52);

(c) in response to the proxy server receiving one of the redirected HTTP request, finding the socket connection to the peer server server (Specification, paragraph 021; see also Figure 3, step 54), translating the HTTP requests into a multiplexed protocol comprising a request packet, and sending the request packet to the peer server (Specification, paragraph 021; see also Figure 3, step 54);

(d) in response to the peer node receiving the request packet, demultiplexing the request, translating the request packet back into the original HTTP request, and passing the HTTP request to a local web server (Specification, paragraph 021; see also Figure 3, step 56);

(e) in response to the peer node receiving an HTTP response from the Web server, translating the HTTP response into a response packet, and sending the response packet to the proxy server over the outbound socket connection (Specification, paragraph 021; see also Figure 3, step 58); and

(f) in response to the proxy server receiving the response packet from the peer server, translating the response packet back into the HTTP response, and sending the HTTP response to the requesting Web browser (Specification, paragraph 021; see also Figure 3, step 60).

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-4 and 17-20 were properly rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,349,336 B1 to *Sit et al.* (hereinafter "*Sit*").

B. Whether claims 5-7, 15, 16, 21-23, and 31-34 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sit*.

C. Whether claims 8, 9, 24, and 25 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sit* in view of U.S. Patent No. 6,917,965 B2 to *Gupta et al.* (hereinafter "*Gupta*").

(7) ARGUMENT

A. Introduction

The Patent Office has not shown where all the elements of the pending claims are shown in the prior art with sufficient particularity to sustain either an anticipation rejection or an obviousness rejection. In particular, the Patent Office has not shown where the prior art discloses the feature of translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall, as recited in the claims. As such, the Appellants request that the Board reverse the Examiner and instruct the Examiner to allow the claims for at least this reason.

B. Summary Of References

1. U.S. Patent No. 6,349,336 B1 To *Sit*

Sit relates to enabling a tunneling action, which allows communication between a remote processor and a local processor when the remote processor is coupled to the local processor via a reverse proxy device. (See *Sit*, col. 8, ll. 54-57). However, *Sit* does not disclose translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall, as recited in the claims. Instead, *Sit* discloses fooling a firewall in order to pass data to a browser, which is behind the firewall. To further illustrate, *Sit* discloses wrapping a request sent from a browser 314E to a web server 308I, which is behind a firewall 305, such that, to the firewall 305, the request appears as a response from the browser 314E to a request sent by the web server 308I. (See *Sit*, col. 7, ll. 50-57). As is well known, wrapping includes a header, which precedes encapsulated data, and a trailer, which follows the encapsulated data, such that the encapsulated data is not viewable to a firewall. Wrapping does not involve translating an HTTP request into a request packet. Therefore, *Sit* does not disclose translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall.

2. U.S. Patent No. 6,917,965 B2 To *Gupta*

Gupta relates to networked client/server systems and methods of annotating multimedia content in networked client/server systems. (See *Gupta*, col. 1, ll. 13-15). Specifically, *Gupta* discloses that users on a network system can annotate a presentation, such as data pertaining to the presentation, and send these annotations via email. (See *Gupta*, col. 1, ll. 55-57 and col. 2, ll. 28-32). Furthermore, *Gupta* discloses that other users may create annotations in response to the initial annotation by replying to the email. (See *Gupta*, col. 2, ll. 49-57). However, *Gupta* does not disclose translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall, as recited in the claims.

C. Legal Standards

1. The Standards For Establishing Anticipation

Section 102 of the Patent Act provides the statutory basis for an anticipation rejection and states *inter alia*:

> A person shall be entitled to a patent unless
> ***
> (e) the invention was described in - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language....

The Federal Circuit's test for anticipation has been set forth numerous times. "It is axiomatic that for prior art to anticipate under 102 it has to meet every element of the claimed invention." *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1379 (Fed. Cir. 1986). This standard has been reinforced. "To anticipate a claim, a reference must disclose every element of the challenged claim and enable one skilled in the art to make the anticipating subject matter." *PPG Indus. Inc. v. Guardian Indus. Corp.*, 75 F.3d 1558, 1577 (Fed. Cir. 1996) (citations omitted). Further, "a finding of anticipation requires that the publication describe all of the elements of the claims, arranged as in the patented device." *C.R. Bard Inc. v. M3 Sys. Inc.*, 157 F.3d 1340, 1349 (Fed. Cir. 1998) (emphasis added and citations omitted).

When determining if a reference shows a claim element, the Patent Office is encouraged to give claim elements their broadest reasonable interpretation consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000); MPEP § 2111. Despite the admonition that the Patent Office interpret the claims broadly, the Federal Circuit has repeatedly stated that the interpretation must be consistent with the specification. *In re Am. Acad. of Sci. Tech Center*, 367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re Thrift*, 298 F.3d 1357, 1364 (Fed. Cir. 2002); *In re Hyatt*; *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997). Furthermore, the Federal Circuit has, on more than one occasion, indicated that reasonableness is determined as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech Center* at 1364; *In re Morris* at 1054; *In re Bond*, 910 F.2d 831, 833 (Fed. Cir. 1990). In addition, words in a claim must be given their plain meaning and "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385 (CCPA 1970).

2. The Standards For Establishing Obviousness

Section 103(a) of the Patent Act provides the statutory basis for an obviousness rejection and reads as follows:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Courts have interpreted 35 U.S.C. § 103(a) as a question of law based on underlying facts. As the Federal Circuit stated:

> Obviousness is ultimately a determination of law based on underlying determinations of fact. These underlying factual determinations include: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) the extent of any proffered objective indicia of nonobviousness.

Monarch Knitting Mach. Corp. v. Sulzer Morat GmBH, 45 U.S.P.Q.2d (BNA) 1977, 1981 (Fed. Cir. 1998) (internal citations omitted).

Once the scope of the prior art is ascertained, the content of the prior art must be properly combined. An obviousness inquiry requires looking at a number of factors, including the background knowledge possessed by a person having ordinary skill in the art, to determine whether there was an apparent reason to combine the elements of the prior art in the fashion claimed by the present invention. *KSR Int'l v. Teleflex, Inc.*, 550 U.S. __, 82 U.S.P.Q.2d (BNA) 1385, 1396 (2007). "Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demand known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, this analysis should be made explicit. See *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness")." *KSR*, 550 U.S. __, 82 U.S.P.Q.2d at 1396 (2007).

While the Patent Office is entitled to give claim terms their broadest reasonable interpretation, this interpretation is limited by a number of factors. First, the interpretation must be consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000); MPEP § 2111. Second, the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *In re Cortright*, 165 F.3d 1353, 1359, (Fed. Cir. 1999); MPEP § 2111. Finally, the interpretation must be reasonable. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1369 (Fed. Cir. 2004); MPEP § 2111.01. This means that the words of the claim must be given their plain meaning unless Appellant has provided a clear definition in the specification. *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989).

If a claim element is missing after the combination is made, then the combination does not render obvious the claimed invention, and the claims are allowable. As stated by the Federal Circuit, "[if] the PTO fails to meet this burden, then the Appellant is entitled to the patent." *In re Glaug*, 283 F.3d 1335, 1338 (Fed. Cir. 2002).

D. Claims 1-4 And 17-20 Are Not Anticipated By *Sit*

Claims 1-4 and 17-20 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Sit*. The Appellants respectfully traverse the rejection.

1. *Sit* Does Not Disclose Translating An HTTP Request Into A Request Packet And Sending The Request Packet To A Peer Server, Which Is Located Behind A Firewall

According to Chapter 2131 of the M.P.E.P., in order to anticipate a claim under 35 U.S.C. § 102, "the reference must teach every element of the claim." The Appellants submit that *Sit* does not teach every element recited in claims 1-4 and 17-20. More specifically, claim 1 recites a method for providing a Web browser running on a computer with access to a peer server located behind a firewall comprising, among other features, in response to a proxy server receiving an HTTP request to access the peer server from the Web browser, "translating the HTTP request into a request packet and sending the request packet to the peer server." Claim 17 includes similar features. The Appellants submit that *Sit* does not disclose or suggest translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall. Instead, *Sit* discloses fooling a firewall in order to pass data to a browser, which is behind the firewall. More specifically, *Sit* discloses wrapping a request sent from the browser 314E to the web server 308I, which is behind the firewall 305, such that, to the firewall 305, the request appears as a response from the browser 314E to a request sent by the web server 308I. (See *Sit*, col. 7, ll. 50-57). As is well known, wrapping includes a header, which precedes encapsulated data and a trailer, which follows the encapsulated data such that the encapsulated data is not viewable to a firewall. Wrapping does not involve translating an HTTP request into a request packet. In fact, *Sit* teaches away from the present invention in that *Sit* discloses fooling a firewall into allowing the transmission of a packet by altering header information such that the packet appears as something it is not, i.e., instead of being a request, the packet appears as a response.

The Patent Office responds to this argument by stating that "the term 'translating the HTTP request into a request packet' under the broadest reasonable interpretation standard does not appear to be limiting in the sense as argued by the applicant." (See Final Office Action, page 2). The Patent Office goes on to state that the plain meaning of the term "translating" is a step to change into another form and the plain meaning of the term "request packet" is any packet including a request by a sender to a destination. (See Final Office Action, page 2). Furthermore, the Patent Office states that a request packet is one translated from an HTTP request and then submitted to a peer server, where the peer server translates the message back to the HTTP request. (See Advisory Action mailed June 2, 2008, page 2). Thus, according to the Patent Office, a translation of an HTTP request into a request packet is any modification to an HTTP request into a packet, where the packet is changed into another form and includes a request from a sender to a destination. (See Final Office Action, page 3). The Patent Office goes on to state that this interpretation is consistent with paragraph **[021]** of the Specification. (See Final Office Action, page 3). The Appellants respectfully disagree for a number of reasons. First, in the interpretation noted above, the Patent Office has ignored all the features recited in claim 1. Specifically, the Patent Office is ignoring the feature of translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall. By stating that "a translation of an HTTP request into a request packet is any modification to an HTTP request into a packet, where the packet is changed into another form, and where the packet includes a request from a sender to a destination," the Patent Office ignores the features of a request packet and sending a request packet. (See Final Office Action, page 3). As mentioned above, according to Chapter 2131 of the M.P.E.P., in order to anticipate a claim under 35 U.S.C.

§ 102, "the reference must teach every element of the claim." By ignoring the feature of a request packet recited in the claims, the Patent Office is ignoring its burden under 35 U.S.C. § 102.

Second, the Patent Office attempts to mask this shortcoming by stating that the interpretation given above is consistent with paragraph **[021]** of the Specification. However, the Appellants submit that the Patent Office is impermissibly broadly construing the features recited in claim 1. According to Chapter 2111 of the M.P.E.P., while claims should be given their broadest reasonable interpretation, the interpretation must be "consistent with the specification." The Appellants submit that the Patent Office is not interpreting claim 1 in a manner that is consistent with the Specification. In particular, paragraph **[021]** of the Specification states the following:

> [021] FIG. 3 is a flow diagram illustrating the process for enabling a Web browser 30 to access the peer server 24' behind a firewall 34. The process begins in step 50 with the peer server 24 registering an outbound socket connection with the proxy server 36. In step 52, all incoming HTTP requests intended for the peer server 24' are redirected to the proxy server 36. In response to receiving a redirected HTTP request in step 54, the proxy server 36 finds the socket connection to the peer server 24', translates the HTTP requests into a **multiplexed protocol comprising a request packet**, and sends the request packet to the peer server 24'. In step 56, the peer node 26 receives the request packet, demultiplexes the request, converts the request packet back into the original HTTP request, and passes the HTTP request to the local Web server 28. In step 58, the peer node 26 receives an HTTP response from Web server 28, converts the HTTP response into a response packet, and sends the response packet to the proxy server 36 over the outbound socket connection. In step 60, the proxy server 36 receives the response packet from the peer server 24', converts the response packet back into the HTTP response, and sends the HTTP response to the requesting web browser 30 (emphasis added).

As shown above, paragraph **[021]** states that the HTTP request is translated into a multiplexed protocol comprising a request packet and sends the request packet to a peer server. Thus, the Specification explicitly states that an HTTP request is translated into a request packet, not just a packet. Therefore, the Appellants submit that the Patent Office is interpreting the feature of, in response to a proxy server receiving an HTTP request to access the peer server from the Web browser, "translating the HTTP request into a request packet and sending the request packet to the peer server" in a manner entirely inconsistent with the Specification.

Third, even assuming *arguendo*, that the Patent Office's interpretation of the feature of translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall, was somehow correct, *Sit* still does not disclose all the features of claim 1, as interpreted by the Patent Office. Specifically, the Patent Office has acknowledged that the claim involves changing the packet into another form. *Sit* does not disclose this feature. As mentioned above, *Sit* involves wrapping a request with a header and a trailer. However, the packet itself is not transformed, or even changed, to use the nomenclature proposed by the Patent Office. For this reason and the reasons noted above, claims 1 and 17 are patentable over the cited reference. Likewise, claims 2-4, and 18-20, which respectively depend from claims 1 and 17, are patentable for at least the same reasons along with the novel features recited therein.

E. Claims 5-7, 15, 16, 21-23, And 31-34 Are Patentable Over *Sit*

Claims 5-7, 15, 16, 21-23, and 31-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sit*. The Appellants respectfully traverse the rejection.

According to Chapter 2143.03 of the M.P.E.P., in order to "establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." The Appellants submit that *Sit* does not disclose all the features recited in claims 5-7, 15, 16, 21-23, and 31-34. As detailed above, *Sit* does not disclose or suggest all the features recited in claim 1 or 17, the base claims from which claims 5-7, 15, 16, 21-23, 31, and 32 ultimately depend. Therefore, these claims are patentable over *Sit* for at least the same reasons noted above with respect to claims 1 and 17.

1. *Sit* Does Not Disclose Translating An HTTP Request Into A Request Packet And Sending The Request Packet To A Peer Server, Which Is Located Behind A Firewall

Claim 33 recites a method for providing a web browser comprising, among other features, in response to a proxy server receiving a redirected HTTP request, "translating the HTTP requests into a multiplexed protocol comprising a request packet, and sending the request packet to the peer server." Claim 34 includes similar features. As detailed above, *Sit* does not disclose translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall.

2. *Sit* Does Not Disclose Translating An HTTP Packet Into A Response Packet And Sending The Response Packet To A Proxy Server

Claim 33 also recites that, in response to a peer node receiving an HTTP response from the Web server, "translating the HTTP response into a response packet, and sending the response packet to the proxy server." Claim 34 includes similar features. The Appellants have reviewed *Sit* and submit that *Sit* does not disclose that in response to a peer node receiving an HTTP response from the Web server, translating an HTTP packet into a response packet and sending the response packet to a proxy server. For at least this reason and the reasons noted above with reference to claims 33 and 34, these claims are patentable over *Sit*.

F. Claims 8, 9, 24, And 25 Are Patentable Over *Sit* In View Of *Gupta*

Claims 8, 9, 24, and 25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sit* in view of *Gupta*. The Appellants respectfully traverse the rejection. The Appellants submit that neither *Sit* nor *Gupta*, either alone or in combination, discloses or suggests all the features recited in claims 8, 9, 24, and 25. As detailed above, *Sit* does not disclose or suggest all the features recited in claim 1 or 17, the base claims from which claims 8, 9, 24, and 25 ultimately depend. Moreover, *Gupta* does not overcome the previously noted shortcomings of *Sit*. Therefore, claims 8, 9, 24, and 25 are patentable over the cited references for at least the same reasons noted above with respect to claims 1 and 17.

G. Conclusion

As set forth above, none of the cited references, either alone or in combination, disclose or suggest the feature of translating an HTTP request into a request packet and sending the request packet to a peer server, which is located behind a firewall, as recited in the claims. As such, the Appellants request that the Board reverse the Examiner and instruct the Examiner to allow the claims.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By:

Anthony J. Josephson
Registration No. 45,742
100 Regency Forest Drive, Suite 160
Cary, NC 27518
Telephone: (919) 238-2300

Date: August 15, 2008
Attorney Docket: 1104-062

(8) CLAIMS APPENDIX

1. A method for providing a Web browser running on a computer with HTTP access to a peer server located behind a firewall in a peer-to-peer network, comprising;

(a) providing the peer-to-peer network with a proxy server;

(b) registering an outbound socket connection with the proxy server by the peer server;

(c) in response to the proxy server receiving an HTTP request to access the peer server from the Web browser, translating the HTTP request into a request packet and sending the request packet to the peer server; and

(d) in response to the peer server receiving the request packet, translating the request packet back into the HTTP request and responding to the request, thereby enabling generic web traffic to flow.

2. The method of claim 1 wherein the peer server further includes a Web server, step (d) further including the steps of:

(i) responding to request,by passing the HTTP request to the Web server;

(ii) receiving an HTTP response from Web server;

(iii) translating HTTP response into a response packet;

(iv) sending the response packet from the peer server to the proxy server over the outbound socket connection;

(v) receiving the response packet on the proxy server and translating a response packet back into the HTTP response; and

(vi) sending the HTTP response from the peer server to the Web browser.

3. The method of claim 2 wherein the peer-to-peer network includes multiple peer servers, and the proxy server is separate and apart from the peer servers.

4. The method of claim 3 further including the step of: providing each of the peer servers with a peer node, a Web server, and a Web browser.

5. The method of claim 4 further including step of: providing the peer-to-peer network with a registration server and a DNS server.

6. The method of claim 5 wherein step (b) further includes the step of: passing a name of the peer server from the peer server to the registration server, and receiving a name and IP address of the proxy server to which it is assigned.

7. The method of claim 6 wherein step (b) further includes the step of: registering by the peer server, the name of the proxy server, and the IP address of the proxy server with the DNS server.

8. The method of claim 7 wherein step (b) further includes the step of: after the peer server registers with the proxy server, notifying a user of the computer via e-mail that content exists on the peer server for viewing, and including a URL of the peer server in the e-mail.

9. The method of claim 8 wherein step (b) further includes the step of: in response to the user clicking on the URL e-mail, the computer contacts the DNS server to determine an identity of the proxy server in which to send the HTTP request.

10. A method of claim 3 further including the step of: providing the proxy server with a servlet thread, a registration manager, a peer manager, a peer MessageBox, and a peer packet manager thread.

11. The method of claim 10 wherein step (c) further includes the step of: receiving the HTTP request as a URL by the servlet thread and using the registration manager to determine if the peer server identified in requesting URL is registered with the peer server, and if so, returning the corresponding peer socket.

12. The method of claim 11 wherein step (c) further includes the step of: creating, by the servlet thread, a peer request packet, and passing the peer request packet to the peer manager.

13. The method of claim 12 wherein step (c) further includes the step of: providing the peer request packet with a MessageBoxID, an HTTP URL, HTTP headers, and an HTTP Post Data field.

14. The method of claim 13 wherein step (c) further includes the step of: finding by the peer manager, the socket connection to the peer server, and passing the peer request packet to the peer server.

15. The method of claim 2 wherein step (d) further includes the step of: breaking the HTTP response into chunks and sending the chunks to the proxy server in successive peer response packets.

16. The method of claim 15 wherein step (d) further includes the step of: providing the peer server with several threads for handling HTTP requests from the proxy server, and multiplexing responses to those requests over the same response socket back to the proxy server.

17. A computer-readable medium containing program instructions for providing a Web browser running on a computer with HTTP access to a peer server located behind a firewall in a peer-to-peer network, the program instructions for;

(a) providing the peer-to-peer network with a proxy server;

(b) registering an outbound socket connection with the proxy server by the peer server;

(c) in response to the proxy server receiving an HTTP request to access the peer server from the Web browser, translating the HTTP request into a request packet, and sending the request packet to the peer server; and

(d) in response to the peer server receiving the request packet, translating the request packet back into the HTTP request and responding to the request, thereby enabling generic web traffic to flow.

18. The computer-readable medium of claim 17 wherein the peer server further includes a Web server, instruction (d) further including the instructions of:

(i) responding to request by passing the HTTP request to the Web server;

(ii) receiving an HTTP response from Web server;

(iii) translating HTTP response into a response packet;

(iv) sending the response packet from the peer server to the proxy server over the outbound socket connection;

(v) receiving the response packet on the proxy server and translating a response packet back into the HTTP response; and

(vi) sending the HTTP response from the peer server to the Web browser.

19. The computer-readable medium of claim 18 wherein the peer-to-peer network includes multiple peer servers, and the proxy server is separate and apart from the peer servers.

20. The computer-readable medium of claim 19 further including the instruction of: providing each of the peer servers with a peer node, a Web server, and a Web browser.

21. The computer-readable medium of claim 20 further including instruction of: providing the peer-to-peer network with a registration server and a DNS server.

22. The computer-readable medium of claim 21 wherein instruction (b) further includes the instruction of: passing a name of the peer server from the peer server to the registration server, and receiving a name and IP address of the proxy server to which it is assigned.

23. The computer-readable medium of claim 22 wherein instruction (b) further includes the instruction of: registering by the peer server, the name of the proxy server and the IP address of the proxy server with the DNS server.

24. The computer-readable medium of claim 23 wherein instruction (b) further includes the instruction of: after the peer server registers with the proxy server, notifying a user of the computer via e-mail that content exists on the peer server for viewing, and including a URL of the peer server in the e-mail.

25. The computer-readable medium of claim 24 wherein instruction (b) further includes the instruction of: in response to the user clicking on the URL e-mail, the computer contacts the DNS server to determine an identity of the proxy server in which to send the HTTP request.

26. A computer-readable medium of claim 19 further including instruction of: providing the proxy server with a servlet thread, a registration manager, a peer manager, a peer MessageBox, and a peer packet manager thread.

27. The computer-readable medium of claim 26 wherein instruction (c) further includes the instruction of: receiving the HTTP request as a URL by the servlet thread and using the registration manager to determine if the peer server identified in requesting URL is registered with the peer server, and if so, returning the corresponding peer socket.

28. The computer-readable medium of claim 27 wherein instruction (c) further includes the instruction of: creating, by the servlet thread, a peer request packet, and passing the peer request packet to the peer manager.

29. The computer-readable medium of claim 28 wherein instruction (c) further includes the instruction of: providing the peer request packet with a MessageBoxID, an HTTP URL, an HTTP headers, and an HTTP Post Data field.

30. The computer-readable medium of claim 29 wherein instruction (c) further includes the instruction of: finding by the peer manager, the socket connection to the peer server, and passing the peer request packet to the peer server.

31. The computer-readable medium of claim 18 wherein instruction (d) further includes the instruction of: breaking the HTTP response into chunks and sending the chunks to the proxy server in successive peer response packets.

32. The computer-readable medium of claim 31 wherein instruction (d) further includes the instruction of: providing the peer server with several threads for handling HTTP requests from

the proxy server, and multiplexing responses to those requests over the same response socket back to the proxy server.

33. A method for providing a web browser with HTTP access to a peer server located behind a firewall in a peer-to-peer network, comprising:

(a) registering an outbound socket connection from the peer server to a proxy server;

(b) redirecting all incoming HTTP requests intended for the peer server to the proxy server;

(c) in response to the proxy server receiving one of the redirected HTTP request, finding the socket connection to the peer server, translating the HTTP requests into a multiplexed protocol comprising a request packet, and sending the request packet to the peer server;

(d) in response to the peer node receiving the request packet, demultiplexing the request, translating the request packet back into the original HTTP request, and passing the HTTP request to a local web server;

(e) in response to the peer node receiving an HTTP response from the Web server, translating the HTTP response into a response packet, and sending the response packet to the proxy server over the outbound socket connection; and

(f) in response to the proxy server receiving the response packet from the peer server, translating the response packet back into the HTTP response, and sending the HTTP response to the requesting Web browser.

34. A computer-readable medium containing program instructions for providing a web browser with HTTP access to a peer server located behind a firewall in a peer-to-peer network, the program instructions for:

(a) registering an outbound socket connection from the peer server to a proxy server;

(b) redirecting all incoming HTTP requests intended for the peer server to the proxy server;

(c) in response to the proxy server receiving one of the redirected HTTP request, finding the socket connection to the peer server, translating the HTTP requests into a multiplexed protocol comprising a request packet, and sending the request packet to the peer server;

(d) in response to the peer node receiving the request packet, demultiplexing the request, translating the request packet back into the original HTTP request, and passing the HTTP request to a local web server;

(e) in response to the peer node receiving an HTTP response from the Web server, translating the HTTP response into a response packet, and sending the response packet to the proxy server over the outbound socket connection; and

(f) in response to the proxy server receiving the response packet from the peer server, translating the response packet back into the HTTP response, and sending the HTTP response to the requesting Web browser.

(9) EVIDENCE APPENDIX

The Appellants rely on no evidence, thus this appendix is not applicable.

(10) RELATED PROCEEDINGS APPENDIX

As there are no related proceedings, this appendix is not applicable.